UNITED STATES OF AMERICA
BEFORE THE NATIONAL LABOR RELATIONS BOARD
Eighteenth Region

POLAR COMMUNICATIONS MUTUAL AID CORPORATION Employer/Petitioner and COMMUNICATION WORKERS OF AMERICA, LOCAL 7304 Union	Case 18-UC-410

DECISION AND ORDER

The Employer filed this petition and seeks to exclude from an existing bargaining unit four employees who it alleges are confidential employees. Three of the employees, Don Pich, Kevin Kargel and James Praska, are part of the internet department. The fourth employee, Kristi Sola, is the backup to the computer network administrator. The Employer does not claim that the four employees at issue act in a confidential capacity to persons who formulate, determine and effectuate management policies in the field of labor relations. Instead, the Employer argues that they regularly have access to confidential information concerning anticipated changes which may result from collective-bargaining negotiations.

The Union contends that the four employees are not confidential employees and should remain in the bargaining unit because they have only theoretical access to confidential information which is insufficient to confer confidential status.

Based on the record, as described below, I conclude that the four employees in dispute are not confidential employees and that this petition should be dismissed.

Under Section 3(b) of the Act, I have the authority to decide this matter on behalf of the National Labor Relations Board. Upon the entire record in this proceeding, I find:

1. The hearing officer's rulings are free from prejudicial error and are hereby affirmed.

2. The Employer is engaged in commerce within the meaning of the Act, and it will effectuate the purposes of the Act to assert jurisdiction herein.[1]

3. The labor organization involved claims to represent certain employees of the Employer.

4. A question affecting commerce exists concerning the representation of certain employees of the Employer within the meaning of Section 9(c)(1) and Section 2(6) and (7) of the Act.

In this Decision, I will first describe the Employer's operation, including an overview of the systems it administers and the bargaining relationship of the parties. Second, I will describe the Employer's internal and external domains as related to its computer system. I will then describe in detail the access that the employees in issue have to the internal and external domains. Fourth, I will briefly describe the uncontested evidence about the Employer's use of e-mail in relation to its labor relations decisions and strategies. Finally, I will explain my conclusion that, under long-standing Board law,

[1] The Employer, Polar Communications Mutual Aid Corporation, is a North Dakota corporation with an office and place of business in Park River, North Dakota, where it is engaged as a telecommunication and ISP provider. During the past 12 months, a representative period, the Employer derived gross revenues in excess of $1 million and purchased and received goods and services valued in excess of $50,000 directly from sources located outside the State of North Dakota.

the four employees at issue are not confidential employees within the meaning of the Act.

THE EMPLOYER'S OPERATION

The Employer operates a telecommunications company that provides cable television service, cell phone access, and internet access to its customers on the worldwide web, along with e-mail, high speed internet and dial-up internet. It serves customers in northeastern North Dakota. Dave Dunning is the Employer's Chief Executive Officer and General Manager and has held this position since 1996. Dunning is responsible for both the technical and financial operations of the company. He reports to a board of directors and is directly involved in labor relations.

Since July 2003, the Employer has used Lynne Webster, an independent contractor, to perform human resources services for Polar Communications. She develops job descriptions; is responsible for advertising for positions; administers the collective bargaining agreement; and is involved in hiring, disciplining, and terminating employees. She does not work in the Employer's place of business, but communicates with Dunning by e-mail, phone and facsimile.

The parties to the instant case have had a bargaining relationship since about 1965. The current collective-bargaining agreement is effective by its terms from January 1, 2003 through December 31, 2005, and the parties have begun negotiations for a successor contract. The Employer's negotiating committee consists of Dunning; Lynne Webster; Karen Johnson, the accounting manager; and Jack McGirl, outside legal counsel. A different negotiating team was in place during the 2002 negotiations.

INTERNAL AND EXTERNAL DOMAINS

Internal Domain

The Employer's internal domain is Polartel.com, which is everything above the firewall. This is the domain where all employee information is stored and where employee e-mails are located. Employee e-mails to each other do not cross the firewall, but stay in the Polartel domain. Once an e-mail leaves the Polartel.com server and is destined for an external server, it travels through the Employer's firewall and on to its destination.

Every employee at the Employer has access to a computer, as well as internet and e-mail access. All employees have their own unique usernames and passwords. Once employees log on to their work stations, they are able to access their own internet and e-mail accounts. With the usernames and passwords, employees can also access a drive on the network server that contains their personal documents that they have saved to the server. The Employer also utilizes a shared driver that can be accessed by all employees of the company.

The Employer's internal e-mail goes through the Polartel.com server. This server and the computer systems that utilize this server are maintained by the computer network administrator, Lisa Whaley. Whaley has held her position for three years. She is not a member of the collective-bargaining unit. She maintains all the computer systems that the employees use, ensures that the systems are working and that the employees have the applications they need and are able to access the internet, read their e-mails, see their calendars, and perform other functions on their computers.

When Whaley is absent from her job her back-up is Kristi Sola. Other than a once a year training, Whaley is not away from the office often on business, although she may be gone occasionally for sick time or a vacation. Sola is a bargaining unit member that the Employer contends should be excluded as confidential.

External Domain

In February 2002, the Employer established an internet operations department whose employees are responsible for customer-based systems, including Polarcom.com, which is an external server administered by the Employer. Whereas the network administrator is responsible for the Polartel.com domain (described above), that provides service to the employees of Polar, including managers and supervisors, the internet operations department's domain is from the firewall of the Employer to the internet. The internet operations department also administers other domains for other companies.

The employees in the internet department are generally responsible for keeping Polar running as an internet service provider (ISP), including the operation, maintenance and upkeep of the systems involved. Internet operations department employees do not have responsibility for the Polartel.com server.

Karl Blake has been the internet operations supervisor since the department's creation. Blake has no involvement in labor strategy. Three additional employees round out the internet operations department and report to Blake. They are Don Pich, James Praska and Kevin Kargel, whom the Employer petitions to exclude as confidential employees. Pich and Praska each hold the title of network specialists-data. Kargel is a network technician-data. Each of the three employees who work in the

internet operations department has access to all the same servers and they all back each other up. The only difference between the network specialists-data and the equipment technician-data is that the network specialists-data completed certain classwork to get the network specialist designation. The parties stipulated that each of the internet department employees has equal access to the systems and essentially the same job duties. Therefore, the employees in these two job classifications will be treated together for purposes of this Decision. The Employer claims that all three should be excluded from the unit as confidential employees.

ACCESS OF EMPLOYEES IN ISSUE

Internal Domain

In her role as network administrator, Whaley uses the domain level administrator username and password which allows access to all programs within the domain. Specifically, this password gives root level access to everything on the domain, similar to the network administrator password used by the internet operations department. Sometimes when Whaley is troubleshooting an employee problem, depending on what it is, she may need the employee's username and password, which she keeps under lock and key. However, she doesn't need the employee's username and password to see the employee's e-mails, as she can use the administrator password.

Sola has worked for Polar for four-and-a-half years. When Whaley is away from the office, Sola serves as her backup and, as such, knows the administrator username and password. She also knows where Whaley keeps the employees' usernames and passwords. Sola needs this access so that she can perform Whaley's job when Whaley is absent. However, it is clear from Whaley that Sola has access only when Whaley is

not in the office. Even Whaley doesn't use usernames and passwords regularly, and in fact described her use as only occasional. The evidence also indicates that, depending on the problem, Sola will let it wait until Whaley returns to the office whenever possible.

The Employer has a surveillance system that records all the e-mails that employees send and receive. With it, it is possible to see what people are doing as they are doing it. Sola has the ability to use the surveillance program and has been shown generally how it works. However, Sola offered unrebutted testimony that she has never used this program.

Sola testified that she knows the administrative password and uses it when she has to look on the server for something, for example if the server goes down or if someone is having trouble with something on the server. She does not have copies of employees' usernames and passwords but knows where Whaley keeps them. She only accesses employee e-mails when troubleshooting. She testified she doesn't like to know the employees' usernames and passwords, and has generally waited until the user is present and can type in their own password.

The evidence establishes that Sola has never accessed Dunning's files, and assumes that she would lose her job for accessing files without specific supervisor permission. She recalls accessing Dunning's e-mail only when he asked her to because of a problem, and then he was present as she accessed his e-mail. The Employer is also clear that Sola has no work-related reason to access anyone's e-mail, let alone Dunning's, unless there is a problem with the e-mail. In fact, were Sola to access e-mails for any other reason, she could be disciplined.

Employer witnesses who testified indicated that they had no reason to believe that Sola has ever used her knowledge inappropriately to access e-mails of the Employer regarding labor relations.

External Domain

According to their job descriptions, the internet department employees are responsible for maintaining current documents of the company's entire internet network, including both hardware and software, for ensuring access to the internet supervisor or appropriate department head in the absence of the internet supervisor; and for ensuring that all products on the system are properly installed and meet licensing requirements. To that end, the employees must document and keep track of the software programs the Employer has on the servers and on the systems and what IOS levels they are at, and they also need to track what passwords are on what machines to access the machines and ensure licensing for the programs that are put on the machines.

Each of the employees in the internet department is able to use the systems administrator password, which allows the employees full rights to perform all functions on any given server or piece of equipment. Specifically, it allows users to manipulate files, look at data in files, run programs, and access e-mails on Polarcom.com – even without individual usernames and passwords. Polarcom.com users are not employees, but may be members of the Employer's board of directors. Only the employees in the internet operations department and the supervisor have this ability. Thus, according to the Employer, the employees have theoretical access to the e-mails of members of the Employer's board of directors.

In addition, the record evidence establishes that the internet operations department employees have access to e-mails from employees that cross the firewall. According to the Employer, with the system administrator password you could access anything on the server, change anything with the system, shut it down and generally cause problems.

The internet operations department employees also have access to a network sniffer to search out different protocols and for use in troubleshooting e-mail problems. The record evidence indicates that the network sniffer hasn't been used to look for Polar employees' e-mails. However, it would be possible to use the network sniffer to capture e-mails sent from an external server to Dunning or from Dunning to an external recipient. The Employer asserts that it would not be possible to prevent the internet department employees from using the network sniffers or administrative passwords and still enable them to do their jobs.

While the Employer can determine whether an employee has used the system administrator password by looking at log files and the commands that they run, it would be more difficult to track whether an employee was using a network sniffer to access e-mail inappropriately. However, the record evidence makes clear that the Employer does not believe, nor does it have any reason to suspect, that any of the employees it claims are confidential have used their heightened access to learn the Employer's confidential labor relations information. In fact, the job descriptions of the employees at issue require that they maintain strict confidentiality of computer records, and of passwords and access to systems.

Pich testified that he does not regularly review customer e-mail. The common types of problems that the internet employees deal with are customer problems with passwords, mailboxes being full and e-mail attachments that are too large for the mailbox. In these circumstances, Pich may have occasion to look at a customer's e-mail, otherwise he would have no real business reason to check e-mail. However, he testified that the department does random checks to see if e-mail accounts are working to verify the health of an e-mail server. Pich has never run across an e-mail from Dunning or a board member during these checks. He also said that if it was obviously a board member's name he would exclude that e-mail from the random check, because, explained Pich, there is a policy at Polar that employees are not to view board members' communications. It appears from the record evidence that the chances of randomly viewing an e-mail from Dunning or a board member would be 1 in 10,000 or less, particularly if the e-mail has already been downloaded and is therefore not on the server anymore. Pich further testified that he would only have access to internally generated e-mails if they were sent to someone on the Polarcom.com server, or possibly another external domain they administer. Pich has never accessed board members' e-mails or any labor strategy notes regarding bargaining with the CWA.

Regarding the network sniffer, Pich testified that he uses a network sniffer or packet sniffer about once every three months or so. He has never used a network sniffer to locate an e-mail from Dunning. The sniffer is able to record live traffic. Depending on what form the packet sniffer is in (hexadecimal code or ASCII (plain language) it may or may not be difficult to read the e-mail. Pich said that he would be subject to discipline if he used a network sniffer to uncover e-mails outside of a normal

business purpose consistent with company policy. He testified that he believes that e-mails are privileged information.

It is Blake's expectation that employees in his department keep any computer records strictly confidential and for business purposes. If he thought they were doing otherwise, he would investigate and possibly discipline them. He also testified that an employee may be asked to help fix an e-mail problem of a board member and then may see other e-mails in the mailbox and that it would be a violation of work rules and confidentiality if the techs were to look at e-mails with no business purpose. However, he testified that it would be possible to run into e-mails from Dunning inadvertently when using the network sniffer to search for specific protocols.

It is also clear from the record that there are other employees of the Employer who potentially have access to confidential labor relations information. For example, Blake, who used to be an equipment technician, testified that equipment technicians have the ability to listen on the phone lines from the central office. Blake indicated that to do so would be unethical and would subject an employee to discipline. He further testified that it would be difficult to detect if phone equipment technicians were listening to Dunning's calls. However, other testimony indicates it may not be very easy to eavesdrop on a phone call because the calls are in real time. Thus, a technician would have to know when a call was being placed and what trunk was being utilized. The phone technicians are in the unit, and the Employer does not contend that they are confidential.

EMPLOYER'S EVIDENCE REGARDING USE OF E-MAILS IN LABOR RELATIONS

The Employer first began using e-mails to discuss labor relations matters during the 2002 contract negotiations. That was also the first time that the Employer had used an outside human resources administrator. The Employer contends that because that person did not work at the Employer it was necessary to use e-mail to communicate about the negotiations. It was also the first time that the Employer's legal counsel, Jack McGirl, and the Employer's board members used e-mail to communicate regarding bargaining.

It was during the 2002 negotiations then that the Employer became aware that certain bargaining unit employees potentially had access to the e-mails of Dunning and others by virtue of their job duties. Specifically, the undisputed evidence establishes that the Employer indicated to the Union that it considered certain people confidential employees, and asked that they be removed from the Unit. The unrebutted record evidence indicates that, ultimately, the parties agreed to put the issue on hold until the contract came up for negotiations again. Therefore, the Union does not contend, and I do not find, that the Employer waived its right to raise the issue of the confidential status of these four employees in dispute.

The record contains several examples of how and why the Employer uses its e-mail system to communicate regarding labor relations matters, including collective bargaining strategizing. For example, Webster testified that she is involved in preparing for negotiations with the Union, and oftentimes that preparation takes place via the internet, although it also includes telephone conferences, and face-to-face meetings. Webster works in Devils Lake, over an hour away from the office where Dunning and

Johnson work. She further testified that e-mail communications are important to strategy and that while she typically communicates directly with Dunning, he might send e-mails to McGirl, Johnson and/or the board of directors.

Further, the Employer's undisputed evidence indicates that without the ability to communicate by e-mail, its ability to strategize regarding collective bargaining negotiations would be seriously hampered. Dunning testified that he keeps the board members apprised of the status of negotiations via e-mail and that the board always has final approval regarding the contract. The Employer offered several documents from the prior negotiations and the current ones that purported to show that confidential labor relations communications take place via e-mail, a point which the Union does not dispute.

LEGAL ANALYSIS AND CONCLUSION

It is important to initially be clear on the limited nature of the Employer's contention. It is the Employer's argument that because the four employees in dispute have the ability to access the Employer's e-mail and internet systems, and because those systems may contain confidential communications regarding labor relations and collective bargaining, therefore, the four employees are confidential and should be excluded from the bargaining unit. It is important to emphasize that there is no evidence that the employees in dispute have in fact accessed confidential information. It is also important to emphasize that there is no evidence that the employees in dispute have any job-related reason to access confidential information regarding labor relations and collective bargaining. Finally, it is important to emphasize that both the Employer and those employees in dispute who testified, are in agreement that if the employees in

dispute did access confidential information, they could be disciplined. Thus, as the Union emphasized in its argument, it is only because the employees in dispute have a theoretical capability of accessing confidential information that the Employer contends they are confidential employees under the Act.

The Board applies a narrow test in making determinations as to whether an employee is "confidential" and should, therefore, be excluded from a bargaining unit. In NLRB v. Hendricks County Rural Electric Membership Corp., 454 U.S. 170 (1981), the Supreme Court affirmed the Board's "labor nexus" test under which only those employees who act in a confidential capacity to persons exercising managerial functions in labor relations matters are deemed to be confidential employees. However, in addition, as the Board indicated in Pullman Standard Division of Pullman Inc., 214 NLRB 762 (1974), employees will also be found confidential if they have regular access to confidential information which, if prematurely disclosed to the union, would prejudice an employer's bargaining strategy in any future negotiations. However, in Inland Steel Co., 308 NLRB 868, 873 (1992), the Board refused to confer confidential employee status on employees responsible for maintaining an employer's confidential computer database on the basis there was no evidence to show that the employees knew the precise terms to which the employer would agree in a collective-bargaining agreement.

In two cases cited by the Employer, there are critical distinctions between them and the instant case. In The Bakersfield Californian, the secretary whom the Board found to be confidential was held so because she had actual access to labor strategy notes. 316 NLRB 1211, 1213 (1995). Importantly, the Board did not rely on the fact that she opened and distributed mail for the department, including personal

correspondence, or the facts that she maintained files on bargaining unit members, typed her boss's notes from disciplinary investigations and bargaining sessions, and *had access to his computer files, including his files on labor relations policy and labor strategy*. (Id.)

Similarly, in E&L Transport Co., 327 NLRB 408, 409 (1998), also relied on by the Employer, the Board, on remand from the 7th Circuit, was specifically charged with deciding whether the confidential secretary at issue had a labor nexus. There the Board found that the executive secretary was a confidential employee for numerous reasons, none of which is present here. Specifically, the Board noted that she assisted in processing grievances and prepared numerous labor-related documents, including correspondence from her boss to the Employer's director of labor relations proposing changes to the collective bargaining agreement in preparation for upcoming negotiations. Id.

In the instant case the Employer presented no evidence that any of the employees at issue has ever had any actual exposure to these or any similar kinds of documents. Instead, the evidence indicates that the employees would have to take purposeful steps with no business purpose to obtain any confidential labor relations information. Moreover, in doing so, these four employees would violate Employer policies and would be subject to discipline. The evidence further establishes that it would be highly unlikely that the employees would inadvertently run across any such information in the performance of their duties.

In conclusion, Board law makes clear that mere access to confidential labor relations material such as personnel files, minutes of management meetings, strike

contingency plans, departmental strategic planning and grievance responses is not sufficient to confer confidential status unless it can be shown that the employees in issue played some role in creating the documents or in making the substantive decision being recorded; or that the employees in issue have regular access to labor relations information before the union or employees involved; or that the employees in issue have access to the precise terms to which an employer may agree in a collective-bargaining agreement. With regard to the four employees in issue in this case, there is no evidence that any of the four have *any* work related access to labor relations information or to the precise terms to which the Employer might agree in collective bargaining, let alone that the four have "regular" access to such information.

Based on the foregoing, I conclude that the network specialists-data, the equipment technician-data and the back up network administrator do not possess the indicia of confidential employees sufficient to be excluded from the bargaining unit. As each of these positions is currently included in the unit, I will dismiss the Employer's petition.

ORDER

IT IS HEREBY ORDERED that the petition filed herein be, and it is, dismissed.[2]

Dated at Minneapolis, Minnesota, this 29th day of December, 2005.

/s/ Marlin O. Osthus

_____

Marlin O. Osthus, Acting Regional Director
Region Eighteen
National Labor Relations Board
330 South Second Avenue, Suite 790
Minneapolis, MN 55401-2221

---

[2] Under the provisions of Section 102.67 of the Board's Rules and Regulations, a request for review of this Decision may be filed with the National Labor Relations Board, addressed to the Executive Secretary, 1099 14th Street NW, Washington, DC, 20570. This request must be received by the Board in Washington by January 12, 2006.

In the Regional Office's initial correspondence, the parties were advised that the National Labor Relations Board has expanded the list of permissible documents that may be electronically filed with the Board in Washington, DC. If a party wishes to file one of these documents electronically, please refer to the Attachment supplied with the Regional Office's initial correspondence for guidance in doing so. The guidance can also be found under "E-Gov" on the National Labor Relations Board web site: www.nlrb.gov.

FORM NLRB-877
(4-84)

UNITED STATES OF AMERICA
BEFORE THE NATIONAL LABOR RELATIONS BOARD

Polar Communications Employer/Petitioner and Communications Workers of America Local 7304 Union	Case 18-UC-410 DATE OF MAILING December 29, 2005

AFFIDAVIT OF SERVICE OF Decision and Order dated December 29, 2005

I, the undersigned employee of the National Labor Relations Board, being duly sworn, depose and say that on the date indicated above I served the above-entitled document*(s)* upon the following persons, addressed to them at the following addresses:

Richard W. Pins, Esq.
Polar Communications
110 Fourth Street East
Park River, ND 58270

Richard W. Pins, Attorney
Leonard, Street and Deinard, P.A.
150 South Fifth Street
Suite 2300
Minneapolis, MN 55402

Al Piker, CWA Nat'l Representative
Communications Workers of America,
Local 7304
4010 West 65th Street, Suite 114
Minneapolis, MN 55435

Stanley M. Gosch, Esq.
Richard Rosenblatt & Associates, LLC
8085 E. Prentice Avenue
Greenwood Village, CO 80111

Daniel J. Byers, President
CWA Local 7304
5212 Belmont Road
Grand Forks, ND 58201

Subscribed and sworn to before me this 8th day of November, 2005.	DESIGNATED AGENT /s/ Olga Bestilny **NATIONAL LABOR RELATIONS BOARD**